SHOWDOWN AT THE OCR CORRAL:
Ten Things You Need to Know
About HIPAA Enforcement
Under the HITECH Act

State of Alabama
Medical Group Management Association
Winter Conference
Birmingham, Alabama
March 7, 2013

D. Brent Wills, Esq.
Gilpin Givhan, PC
www.gilpingivhan.com
@GG_HealthLaw
1. OCR means business.

- Exponentially increased penalties under HITECH – up to $1.5M per violation
- 3 $1M+ settlements in 2012 (Mass Eye & Ear, Alaska DHHS, BCBSTN)
- Substantially expanded OCR’s enforcement web – to include business associates (“BAs”) and their subcontractors (beginning September, 2013)
- OCR commenced HIPAA compliance audits in 2011 – under contract with KPMG
- OCR leveraging breach notification rule for enforcement – Mass Eye & Ear, Alaska DHHS, BCBSTN all self-reported breaches
- OCR investigates every “major” breach notification it receives (i.e., 500+ affected individuals)
- OCR: Future enforcement will be funded by recoveries.
- HITECH also authorized State AGs to enforce HIPAA (e.g., Massachusetts)

OCR Director: HITECH increased OCR’s workload by 500%.
2. Your HIPAA Enforcement mindset: Not if, but *when*.

- **Epidemic of data breaches** – 77,000+ reported breaches
- 90%+ hospitals experienced breach during 2011-2012; nearly 50% experienced *at least five* breaches
- Occur most often at physician practices – 3 out of 4 “major” breaches reported in Alabama.
- **Phoenix Cardiac Surgery, P.C.** – OCR resolution agreement with *two* physician practice
- **Hospice of Northern Idaho** – self-reported breach; only 441 patients affected
- Health care “elite” (e.g., Emory Hospital; Mass Eye & Ear / Harvard; Stanford Hospital; UCLA Hospital; M.D. Anderson)
- **KPMG breach(es)** – HIPAA auditor caused two “major” hospital breaches
- **CMS** – at least 14 known breaches

**OCR Director:** “. . . regardless of size, covered entities [and BAs, and subcontractors] must take action and will be held accountable for safeguarding [PHI].”
3. Even without penalties, data breaches may be hugely expensive.

- Breach “response” typically entails internal investigation, patient notifications, mitigation of harm, corrective actions
- OCR investigates *every* “major” breach report it receives (and some non-major breaches)
- May necessitate legal assistance, IT specialists, PR consultants / notification specialists, etc.
- Health care industry spends $7B / year dealing with data breaches
- Costs to resolve breaches may by $100s (or $1,000s) per affected patient (e.g., BCBSTN)
- OCR also *publicizes* every major breach report it receives on its “Wall of Shame.”

*What comes next?* Whistle blowers; Class action lawsuits
4. Most breaches are self-inflicted.

- Most common causes:
  - **Lost / stolen unencrypted devices**
    - 80%+ of physicians / staff use smart phones, laptops, other mobile devices – less than 50% are encrypted
  - **Workforce errors**
    - Mistakes (e.g., Mass General -$1M)
    - “Snoopers” and “Peepers” (e.g., UCLA - $865K)
    - Social media
  - **Criminal attacks** – very often “inside jobs”
    - Street value of medical identity may be **up to 50 times greater** than a SSN (e.g., Alabama hospital)
- 25%+ involve paper PHI
- Vs. “hacking” – less than 10% (but . . .)

**OCR Director:** “A lot of these cases turn on some kind of human frailty - people losing things, permissions getting stolen, information getting misused for either fraud or to embarrass somebody else.”

- Confirmed that BAs and their subcontractors must comply with HIPAA – or be subject to OCR enforcement.
- Changes to Privacy Rule:
  - Additional restrictions “remunerated” marketing communications / “sales” of PHI
  - Expanded individuals’ ability to access / control their own PHI
  - Revisions to NPPs and BAAs (see below re: “grandfather” rule)
  - Disclosures to persons involved in an individual’s care; disclosures of student immunizations; maintaining deceased patients’ records
- Update BAAs (unless “grandfathered,” then + 1 year) – including between BAs and subcontractors.
- OCR must investigate the possibility of “willful neglect” (regardless of size of breach) and may bypass informal resolution in such cases.

OCR Director: HITECH enacts “most sweeping changes . . . since [HIPAA was] first implemented.”
6. There are steps you can take to protect yourself against HIPAA enforcement.

- Before a breach:
  - Perform a **security risk analysis** . . . yesterday.
  - Develop a HIPAA compliance program based on security risk analysis.
  - *Regularly* evaluate policies and procedures and safeguards – and promptly take corrective actions, as needed.
  - Have a plan and a team in place *now* to respond to a data breach.
  - *Regularly* train your people – and **hold them accountable**.
  - Note OCR areas of emphasis – e.g., mobile devices, access controls / audit monitoring, contingency plans.
  - Consider cyber insurance

- When a breach occurs:
  - *Immediately* commence internal investigation.
  - Notify every affected individual *without unreasonable delay* – **don’t** rely on 60-day outside limit.
  - If 500+ individuals affected, (i) must immediately notify OCR; and (ii) may be required to give public notice (e.g., press release).

- **Document compliance!**

  *OCR Director:* “Huge points for the entity that acts decisively to deal with . . . the root cause of the breach.”
7. Your HIPAA compliance mindset: It’s your processes, stupid!

- Breaches *will* occur; goal is to demonstrate (i) *reasonable* diligence; and (ii) HIPAA violations, *if any*, were *not* the result of *willful neglect*.

- **OCR resolution agreements** focused on breakdowns in *compliance processes* – i.e., steps CE took (or didn’t take) to prevent, detect, mitigate and respond to breach.

*OCR Director:* “One thing we're going to keep emphasizing is it's that menu of *common-sense steps*, *not* a particular technological solution.”

- HIPAA compliance processes should be:
  - Proactive – *you* must take the initiative
  - Ongoing – must *regularly* evaluate policies and procedures and safeguards, and promptly take corrective actions
  - Organic – should be constantly *evolving* to reflect changes in your circumstances, technology, etc.
  - Integrated – all steps *consistent* with each other

*OCR Director:* “At the end of the day, *it comes down to leadership*: Owning compliance issues and doing so consistently.”
8. OCR really, really wants you to encrypt your mobile devices.

- All three Alabama physician practices on OCR “Wall of Shame” experienced theft / loss of unencrypted mobile devices
- Health care “elite” all experienced breaches that involved theft / loss of unencrypted mobile devices
- HONI, Mass Eye & Ear, Alaska DHHS, BCBSTN all involved theft / loss of unencrypted mobile devices
- OCR published specific guidance to address privacy and security issues relating to mobile devices

*And, by the way . . .*

- Encryption exempts CE from breach notification rule
- Must “address” encryption to qualify for M/U incentives (and avoid Medicare penalties)

**BAs beware!**

- BAs and subcontractors must comply with HIPAA similarly to CEs (e.g., policies and procedures, safeguards, training) – or be subject to OCR enforcement
- BAs will be subject to future HIPAA audits

**Beware your BAs!**

- Data breaches very often involve / caused by BAs
- Is BA your agent? If so, CE may be liable for BA violations.
- Vet your BAs (e.g., cyber insurance, reported breaches)
- Ensure BAAs include adequate protections (e.g., reps and warranties, indemnification)
10. HIPAA audits will continue, but details not clear.

- OCR / KPMG recently completed initial, “pilot” round of 115 audits
- OCR expected to publish audit results and additional guidance – previously published audit protocol.
- OCR Presentation – results from first 20 HIPAA audits – high incidence of non-compliance in access controls / audit monitoring and contingency plans.
- Not clear what form future audits will take, nor whether / when there will be any expansive rollout of audit program.
Numerous resources are available to assist you in complying with HIPAA.

- Guide to HIPAA Privacy and Security of Health Information
- Your Mobile Device and Health Information Privacy and Security
- HIPAA Audit Protocol / OCR Presentation – results from first 20 HIPAA audits
- HIPAA Enforcement – Case Examples & Resolution Agreements
- “Omnibus” HITECH Final Rule
- Sample Business Associate Agreement Provisions (incorporating HITECH modifications)
- Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Also...

- Email me to receive Client Alerts and other important updates!
- Follow the Gilpin Givhan Health Care Practice Group on Twitter!
- Read my article on HIPAA enforcement: It’s 2 AM: Do You Know Where Your Patients’ Information Is?
Any Questions?

D. Brent Wills, Esq.
Gilpin Givhan, PC
bwills@gilpingivhan.com
@GG_HealthLaw

2660 EastChase Lane, Suite 300
Montgomery, Alabama  36117
(334) 244-1111  (phone)
(334) 244-1969  (fax)

3595 Grandview Parkway, Suite 400
Birmingham, Alabama  35243
(205) 547-5540  (phone)
(205) 547-5621  (fax)